

[Sign in](#)
[Web](#) [Images](#) [Groups](#) [News](#) [Froogle](#) [Local](#) [more »](#)

iso 9796

[Search](#)
[Advanced Search](#)
[Preferences](#)
WebResults 1 - 10 of about 115,000 for **iso 9796**. (0.58 seconds)**RSA Security - Recent Results on Signature Forgery**

A weakness has been found in the ISO 9796 signature standard using RSA. ...

Attacks on ISO 9796-2 and slightly modified ISO 9796-1 ...

www.rsasecurity.com/rsalabs/node.asp?id=2090 - 23k -[Cached](#) - [Similar pages](#)**Sponsored Links****Download ISO Standards**The complete ISO collection
organized in 43 categories.
webstore.ansi.org**[PPT] RSA Digital Signature Standards**File Format: Microsoft Powerpoint 97 - [View as HTML](#)**ISO/IEC 9796-2** (Digital Signature Scheme Giving Message Recovery ...)

Provably secure design; To be included in IEEE P1363a; ISO/IEC 9796-

2 to be revised to ...

www.rsasecurity.com/rsalabs/staff/bios/bkaliski/publications/other/kaliski-rsa-signatures-rsa-2000.ppt - [Similar pages](#)**Cryptomathic Technical Articles - New attacks on ISO 9796-1 & -2**

This year, we have seen an ever-increasing list of attacks on ISO 9796-1 & -2, initiated by JS Coron, D. Naccache and J. Stern on ISO 9796-2, ...

www.cryptomathic.com/company/newattacks.html - 19k - [Cached](#) - [Similar pages](#)**Syntax Version 4 ; 40102; 03B - Code list 0591****ISO 9796 #1 padding.** Message padding for digital signature schemes according to ISO 9796 part 1. 7. **ISO 9796 #2 padding.** Message padding for digital ...www.gefeg.com/jswg/cl/v41/40102/cl1d.htm - 20k - [Cached](#) - [Similar pages](#)**ISO - International Organization for Standardization**

ISO/IEC 9796-2:2002 specifies three digital signature schemes giving message recovery, two of which are deterministic (non-randomized) and one of which is ...

www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=35455 - 41k -
[Cached](#) - [Similar pages](#)**Citations: ISO 9796-1 and the new forgery strategy - Coppersmith ...**

D. Coppersmith, S. Halevi, and C. Jutla. ISO 9796-1 and the new forgery strategy.

Unpublished manuscript, 1999.

citeseer.ist.psu.edu/context/1235493/0 - 15k - [Cached](#) - [Similar pages](#)**Multisignature algorithms for ISO 9796**

ISO 9796 is specified for a single signer only. This letter explains how ... 8 ISO, <i>9796

ISO Data Cryptographic Technique -- Digital Signature Scheme ...

portal.acm.org/citation.cfm?id=250023&dl=GUIDE&coll=GUIDE&CFID=73264672&CFTOKEN=6641950 - [Similar pages](#)**'RSA Digital Signature and ISO 9796' - MARC**

Subject: RSA Digital Signature and ISO 9796 From: "Hellan,Kim KHE" <khe () kmd ! dk>

Date: 2001-08-31 14:32:16 [Download message RAW] I have a digital ...

marc2.theaimsgroup.com/?l=openssl-users&m=99927205717972&w=2 - [Similar pages](#)**[PDF] Cryptanalysis of Countermeasures Proposed for Repairing ISO 9796-1**File Format: PDF/Adobe Acrobat - [View as HTML](#)

cache and Stern described an attack on a slight modification of ISO 9796- ... ISO 9796-1